Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

Jason "Jay" O. Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
An V. Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CHRISTINE RIGANIAN and DONNA SPURGEON, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

LIVERAMP HOLDINGS INC. and LIVERAMP INC., *corporations organized under the laws of the State of Delaware*,

Defendants.

Case No. 4:25-cv-00824 (JST)

PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO LIVERAMP'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

Judge: Hon. Jon S. Tigar

Date Action Filed: January 24, 2025

Trial Date: Not set

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES

Page

TABLE OF AUTHORITIES

Page

TABLE OF AUTHORITIES

Page

TABLE OF AUTHORITIES

Page

TABLE OF AUTHORITIES

Page

Statutes

Court Rules

Treatises

TABLE OF AUTHORITIES

Page

Other Authorities

Constitutions

I. INTRODUCTION

Plaintiff class representatives are concerned and injured citizens who allege that LiveRamp's data surveillance and identity resolution infrastructure presents an egregious and serious invasion of privacy interests long recognized in our society through the common law, and well-established in Constitutional law and statutory law. Plaintiffs Riganian and Spurgeon, representing three putative classes,[1] allege that LiveRamp collects extensive personal information from both online and offline sources—including browsing activity, communications content, and sensitive identifiers like Social Security numbers—which it links to unique "RampIDs" associated with each person, and then packages into detailed personal profiles. The data in these profiles, including intimate details about individuals' health, finances, political beliefs, and personal characteristics, are further sold through LiveRamp's Data Marketplace to third parties. Plaintiffs assert claims under California's Constitution, common law invasion of privacy, the California Invasion of Privacy Act (CIPA), the Electronic Communications Privacy Act (ECPA), and for unjust enrichment and declaratory relief.

LiveRamp's motion to dismiss fails both procedurally and on the merits. Having conceded that Plaintiffs state viable privacy claims regarding LiveRamp's "Attribute Enrichment" services, LiveRamp attempts a piecemeal attack on the remaining allegations—a strategy foreclosed by settled law holding that Rule 12(b)(6) does not permit partial dismissal of only portions of a claim. Counts I, II, and VI must proceed in full for this reason alone.

On the merits, LiveRamp's arguments ignore the well-developed jurisprudence in this Circuit recognizing that the surreptitious aggregation and commercialization of vast quantities of personal information can constitute a serious invasion of privacy, even where individual data points might be publicly available or not otherwise protectable. Plaintiffs' allegations mirror those that the Ninth Circuit and courts in this District have found sufficient to state privacy claims against other data aggregators, including data brokers like LiveRamp. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.* ("*Facebook Tracking*"), 956 F.3d 589, 601 (9th Cir. 2020); *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 940 (N.D. Cal. 2023). In *Katz-Lacabe v. Oracle*, Judge

[1] Plaintiffs propose a United States Class, an ECPA and CIPA Sub-Class, and a California Sub-Class. *See* ECF 32, First Amended Complaint ("FAC"), at ¶164.

Seeborg held that allegations of functionally identical conduct—identity resolution services combined with an expansive data marketplace providing access to detailed personal information—plausibly stated violations of plaintiffs' reasonable expectation of privacy. LiveRamp's attempt to distinguish that case fails, particularly given LiveRamp's own representations that it offers a "seamless" transition from Oracle's now-defunct services to its own.

LiveRamp's remaining arguments fare no better. Its partial Section 230 defense fails because LiveRamp is not a passive intermediary but a creator, curator, and seller of its own "bespoke" data products. Its California Consumer Privacy Act (CCPA) preemption argument has been rejected by every court to consider it, as the statute explicitly establishes a floor, not a ceiling, for privacy protections. Its challenges to Plaintiffs' wiretapping claims call for improper fact-finding, and ignore controlling Ninth Circuit precedent and well-pleaded allegations of real-time data interception and analysis. LiveRamp's perfunctory challenges to Plaintiffs' unjust enrichment and declaratory judgment claims fail as well. The motion should be denied.

A. LiveRamp's Conduct

The detailed allegations in the FAC set forth the relevant background for consideration. This includes details drawn from LiveRamp's own technical documentation, regulatory filings, and forensic investigations, setting forth how LiveRamp operates a surveillance enterprise that constructs and monetizes "identity profiles" tied to virtually every adult in the U.S. LiveRamp assigns a unique, persistent "RampID"—analogous to an online Social Security number—to each individual, which it then links to vast quantities of personal information from online and offline sources. FAC ¶¶ 51-93. This includes names, addresses, phone numbers, email accounts, device identifiers, and highly sensitive data such as driver's license and Social Security numbers that allow LiveRamp and its "partners" and clients to track individuals across digital and physical spaces, in real time, indefinitely. *Id.*

LiveRamp's Data Marketplace, a central component of this surveillance infrastructure, facilitates the commodification and sale of highly sensitive personal information, including demographic, behavioral, and "psychographic" attributes—such as race, religion, income, health status, sexual orientation, and political beliefs. *Id.* ¶¶ 94-107. LiveRamp packages this data into

"bespoke" and "custom" "segments" associated with individuals' RampIDs, enabling advertisers and data buyers to target individuals based on highly specific and intimate characteristics. *Id.* ¶¶ 113-131. These segments are sold or made available to a wide array of actors, without the knowledge or consent of the people profiled. The Data Marketplace enables both direct sales and downstream data dissemination through LiveRamp's vast network of data broker and advertising partners. *Id.* ¶¶ 94-112. Additionally, LiveRamp's tracking mechanisms—cookies, pixels, and JavaScript tags—intercept the contents of Plaintiffs' communications with websites revealing what products they searched for and webpages they viewed. *Id.* ¶¶ 18-27, 74-79. These communications are then transformed into actionable data, categorized into segments revealing detailed and sensitive information, which can be sold via LiveRamp's Data Marketplace. *Id*; *see also* ¶¶ 94-112.

These services thus allow LiveRamp and third parties to conduct continuous, invisible surveillance and to buy and sell detailed and sensitive Class member data to advertisers, data brokers, and other third parties. Plaintiffs allege that LiveRamp conducts this surveillance of their online and offline activity without their knowledge or consent. *Id.* ¶¶ 149-163.

B. Plaintiffs Riganian and Spurgeon

Plaintiffs Riganian and Spurgeon each received from LiveRamp, prior to the filing of this lawsuit, a Subject Access Request ("SAR") that partially revealed the scope and detail of LiveRamp's data collection and dissemination practices. *Id.* ¶¶ 14-17, 30-32. The SARs provided to both Plaintiffs contained hundreds to thousands of data points, including names, addresses, phone numbers, email addresses, device identifiers, and other unique personal information accumulated over decades. *Id.*

Plaintiff Riganian's SAR revealed that the company had amassed a vast identity profile on her. It showed that LiveRamp maintained records of nearly every address where she had lived since 1992 and every phone number associated with her over the past twenty years. *Id.* ¶ 14. It also included years' worth of electronic identifiers, such as email addresses she had used for at least two decades. *Id.* LiveRamp had collected and linked over six hundred cookies and unique device identifiers, as well as more than one hundred unique mobile advertising IDs associated with her devices. *Id.* Additionally, the SAR demonstrated that LiveRamp had gathered hundreds of "Custom

IDs" from various partners—identifiers typically assigned when creating accounts with third parties like social networks or retailers—further enriching her dossier. *Id.* The SAR also contained a log of over 1,800 instances in the past four years where LiveRamp pixels were deposited on her devices, with the majority occurring in the last year, indicating near-daily tracking. *Id.* Due to the obfuscated nature of the data, Plaintiffs could not determine the specific websites or apps involved, but these pixels likely represent instances of LiveRamp's wiretapping mechanisms at work. *Id.*

Plaintiff Riganian's SAR further included a file titled "ThirdPartyAccessList," which listed at least 62 third parties with whom LiveRamp had shared or sold her personal information. These third parties included entities such as pharmaceutical companies AbbVie, ad tech firm Freewheel, Google, Amazon, Microsoft, and other data brokers like Lotame and IRI. *Id.* The SAR also disclosed that LiveRamp had collected and associated with Plaintiff Riganian's profile highly sensitive information, including her social security number and driver's license data, and had assigned her persistent "RampIDs"—unique identifiers used to track and profile her. *Id.* ¶¶ 16-17.

Plaintiffs also allege specific examples of websites where LiveRamp's trackers surveilled them. Contrary to LiveRamp's representation that Plaintiffs merely allege visits to top-level domains, Plaintiffs assert that LiveRamp's tracking mechanisms were present on and actively intercepted their communications with specific websites, including the URLs of the specific pages on websites they browsed.[2] *Id.* ¶¶ 20-27. For Plaintiff Riganian, these included articles on health-related sites such as Healthline.com, CVS.com, Health.usnews.com, and Goodrx.com. *Id.* ¶ 26. The FAC details that, for example, when Plaintiff Riganian visited CVS.com to view information on specific medications, LiveRamp intercepted and transmitted the full URL—including the specific product viewed and associated health categories—to its servers. *Id.* ¶¶ 22-25. This allowed LiveRamp to associate her browsing activity with sensitive health-related segments and categories, which could then be made available for sale through its Data Marketplace. *Id.* Plaintiffs make analogous allegations with respect to Plaintiff Spurgeon. *Id.* ¶¶ 29-38.

Plaintiffs also allege that LiveRamp's Data Marketplace offers for sale highly sensitive and

[2] The FAC specifically notes that the trackers collect "full URL[s]"; the FAC lists only the top-level domains for websites (and an exemplar URL for CVS that is "substantially similar" to one browsed by Riganian) out of respect for plaintiffs' privacy and to avoid unnecessary under-seal filing. *See, e.g., id.* n.14-15.

detailed personal information about them, but that they cannot know the full extent or nature of the specific information that has been bought or sold through LiveRamp's services. *Id.* ¶¶ 28, 38. The SARs and LiveRamp's own documentation confirm that Plaintiffs' profiles were made available to a wide array of third parties, but the precise data elements and the downstream uses of their information remain unknown to Plaintiffs due to the opaque and complex nature of LiveRamp's surveillance infrastructure. *Id.* ¶ 112.

II. ARGUMENT

The Court must accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party. *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029-30 (9th Cir. 2009). "If there are two alternative explanations, one advanced by defendant and the other advanced by plaintiff, both of which are plausible, [a] plaintiff's complaint survives a motion to dismiss under Rule 12(b)(6)." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011).

A. LiveRamp's Failure to Challenge the Entirety of Counts I, II, and VI Necessitates Denial of the Motion to Dismiss those Claims

LiveRamp seeks to dismiss only portions of Plaintiffs' Counts I, II, and VI, explicitly conceding that these claims should proceed with respect to "Attribute Enrichment."[3] *See* Mot. at 2 ("because the allegations about Attribute Enrichment allege that LiveRamp has de-pseudonymized data, LiveRamp is not moving to dismiss Counts I, II, or VI, as related to that product"); *id.* at 25 (the Court should "dismiss Plaintiffs' Sixth Cause of Action (except as to Attribute Enrichment)"); Dkt. 49-6 ([Proposed] Order) (requesting that the Court dismiss "the claims apart from Attribute Enrichment"). This strategic choice[4] to challenge only portions of these claims is fatal to LiveRamp's motion under Federal Rule of Civil Procedure 12(b)(6).

[3] Through its "Third-Party Attribute Enrichment" service, LiveRamp allows clients to send it non-anonymized identifying information about particular people, and receive back from LiveRamp a dossier containing all information about that person on the Data Marketplace. FAC ¶¶ 108-110.

[4] LiveRamp's reasons for declining to challenge Plaintiffs' privacy claims "with respect to" Attribute Enrichment, as opposed to any other aspect of LiveRamp's allegedly invasive conduct, are opaque. Given LiveRamp's surveillance infrastructure is designed precisely to "de-pseudonymiz[e] data," *i.e.* to connect online activity and data with real-world offline identities, its apparent agreement that Attribute Enrichment, if it functions as alleged, invades class members' privacy, redounds to the remainder of Plaintiffs' allegations as well.

It is settled law that partial dismissal of a claim is not permissible under Rule 12(b)(6). Courts within this Circuit and elsewhere are univocal on this point: "[b]y its own terms, there does not appear to be any way to grant partial dismissal of a claim under Fed. R. Civ. P. 12(b)(6)." *Sequeira v. United States Dep't of Homeland Sec.*, 2024 WL 2261939, at *2 (N.D. Cal. May 16, 2024) (citation omitted). Rule 12(b)(6) "should not be used on subparts of claims; a cause of action either fails totally or remains in the complaint." *In re Netopia, Inc., Sec. Litig.*, 2005 WL 3445631, at *3 (N.D. Cal. Dec. 15, 2005). A motion to dismiss under Rule 12(b)(6) "doesn't permit piecemeal dismissals of parts of claims; the question at this stage is simply whether the complaint includes factual allegations that state a plausible claim for relief." *BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015); *see also Pinnacle Ventures LLC v. Bertelsmann Educ. Servs. LLC*, 2019 WL 4040070, at *3-4 (N.D. Cal. Aug. 26, 2019) (noting defendant presented no "authority permitting a motion for partial dismissal of claims under Rule 12(b)(6)"); *Fed. Trade Comm'n v. Facebook, Inc.*, 581 F. Supp. 3d 34, 60 (D.D.C. 2022) (noting "a chorus of other courts has held that a 'motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of parts of claims.'"); Wright & Miller, § 1358 Motions to Dismiss—Illustrative Cases, 5B Fed. Prac. & Proc. Civ. § 1358 (4th ed.) ("[A] Rule 12(b)(6) motion may not be used to dismiss only part of a claim.") (collecting cases). Plaintiffs are aware of no authority allowing a defendant to seek to dismiss only portions of a claim at the pleadings stage. *Franklin v. Midwest Recovery Sys., LLC*, 2020 WL 3213676, at *1 (C.D. Cal. Mar. 9, 2020) ("Moving Defendants are asking the Court to dismiss only part of a claim. Moving Defendants may not do so; Federal Rule of Civil Procedure 12(b)(6) does not provide a mechanism for dismissing only a portion of a claim.").

Where a defendant admits a claim can proceed under a portion of the facts alleged, "[t]hat is the end of the matter" at the pleadings stage. *Adjaye v. Cook*, 2024 WL 647636, at *3-4 (N.D. Cal. Feb. 15, 2024). LiveRamp explicitly concedes that Counts I, II, and VI should proceed with respect to Attribute Enrichment, and anticipates "moving for summary judgment on any claim concerning that product after appropriate discovery." Mot. at 2. By operation of Rule 12(b)(6), these Counts necessarily survive in their entirety. *Griffith v. TikTok, Inc.*, 697 F. Supp. 3d 963, 974 (C.D. Cal. 2023) (allowing CIPA claim to proceed on one factual basis without analyzing others,

because "Rule 12(b)(6) 'does not provide a mechanism for dismissing only a portion of a claim.'"); *see also Fed. Trade Comm'n v. Nudge, LLC*, 430 F. Supp. 3d 1230, 1246 (D. Utah 2019) ("[I]f Defendants wish to challenge only parts of Plaintiffs' claims, such a challenge would be appropriate at summary judgment.").

Moreover, even assuming partial dismissal were permissible, it would be nonsensical in this context. As a factual and practical matter, Attribute Enrichment cannot be partitioned off from Plaintiffs' other allegations in the FAC. Attribute Enrichment is inextricably intertwined with LiveRamp's invasive conduct, and just one of a bundle of interrelated services within its surveillance infrastructure. FAC ¶ 108-110. It allows clients to send it plainly identifiable information such as names, addresses, phone numbers, and email addresses, and receive back from LiveRamp a dossier containing all of the information about that particular person available on the Data Marketplace, including "sweeping information about those individuals, including what style car they drive, details about their occupation, health, relationship status, finances, and shopping habits." *Id.* ¶ 109. These "highly detailed, personal, and sensitive 'psychographic' profiles" exemplify the invasiveness of LiveRamp's conduct as described throughout the FAC, but are not alleged by Plaintiffs to be a stand-alone basis for liability. *Id.* ¶ 110. The same core issues—the extent and invasiveness of LiveRamp's data collection and aggregation through identity resolution, and the combination of that conduct with the data available on the Data Marketplace—remain at issue regardless of which specific LiveRamp service is considered. *Id.* LiveRamp's minimal explanation of its reasoning provides no argument to the contrary. Because it does not challenge the entirety of Counts I, II, and VI, they stand in their entirety, both practically and as a matter of law. *Redwind v. W. Union, LLC*, 2019 WL 3069864, at *4 (D. Or. June 21, 2019) ("[C]ourts may not dismiss only some of the claim's allegations if the claim otherwise survives.").[5]

B. Plaintiffs' Invasion of Privacy Claims Stand

LiveRamp's motion also fails on the merits. To establish a privacy claim under the

[5] Because LiveRamp's motion is an explicit "attempt to test the sufficiency and/or substantive merit" of portions of the claims, striking the allegations under Rule 12(f) is likewise improper. *Yarber v. Kia Am., Inc.*, 2023 WL 2654186, at *5 (N.D. Cal. Mar. 27, 2023); *Yamamoto v. Omiya*, 564 F.2d 1319, 1327 (9th Cir. 1977) ("Rule 12(f) is neither an authorized nor a proper way to procure the dismissal of all or a part of a complaint.").

California Constitution, a plaintiff must demonstrate: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest." *Matthews v. Apple, Inc.*, 2024 WL 5517089, at *5 (N.D. Cal. Dec. 20, 2024) (Tigar, J.) (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994)). The California Constitution was amended in 1972 to add an inalienable right to privacy specifically to protect against the advancing encroachments of computerized surveillance and the development of invasive digital "cradle to grave profiles"—precisely the conduct LiveRamp is accused of. *See* Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).[6] To state a common law invasion of privacy claim, a plaintiff must allege "(1) intrusion into a private place, conversation or matter (2) in a manner *highly offensive to a reasonable person*." *Matthews*, 2024 WL 5517089, at *5 (citing *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998)). Both claims are properly alleged.

1. Plaintiffs Have Alleged a Reasonable Expectation of Privacy

LiveRamp fundamentally mischaracterizes the gravamen of Plaintiffs' complaint by arguing that Plaintiffs should have no reasonable expectation of privacy in each individual piece of data LiveRamp has compiled. This argument ignores well-developed jurisprudence establishing that the aggregation of large quantities of data can itself constitute a violation of the reasonable expectation of privacy, even when individual data points might not otherwise be protectable. A reasonable expectation of privacy is violated where a defendant gains "unwanted access to data by electronic or other covert means, in violation of the law or social norms." *Facebook Tracking*, 956 F.3d at 601-02 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). "The question is not necessarily whether Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself. Rather, we must examine whether the data itself is sensitive *and* whether the manner it was collected" violates social norms. *Id.* at 603.

As LiveRamp recognizes in devoting several pages of its brief attempting to distinguish it,

[6] *See also* Nicole A. Ozer, *Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age*, 39 BERKELEY TECH. L.J. 963, 1025-26 (2024) ("[H]ow [data brokers] collect, use, sell, and trade, information for profit" is "exactly the type of privacy harm of 'cradle-to- grave' dossiers that the California constitutional right to privacy was passed to protect against.").

Facebook Tracking directly controls this case. There, plaintiffs alleged that Facebook obtained "an enormous amount of individualized data" by collecting URLs of third-party websites that could potentially "divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform," thereby gaining "cradle-to-grave profile[s]" of internet users without their consent. *Id.* at 603, 605. Because Facebook garnered "a comprehensive browsing history of an individual," allowing Facebook to "compile a 'vast repository of personal data,'" the court held that Facebook allegedly compiled "highly personalized profiles from sensitive browsing histories and habits," preventing any conclusion that the Plaintiffs failed to allege a reasonable expectation of privacy. *Id.* at 603, 604 n.7 (citing *Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018); *Riley v. California*, 573 U.S. 373, 397-99 (2014)). The Ninth Circuit emphasized that under controlling precedent, "individuals have a reasonable expectation of privacy in collections of information that reveal 'familiar, political, professional, religious, and sexual association'" and that "individuals maintain the expectation that entities will not be able to collect such broad swaths of personal information absent consent." *Id.* at 604 n.7.

District courts have consistently applied *Facebook Tracking* to find reasonable expectations of privacy in aggregated data. In *Katz-Lacabe v. Oracle*, the court confronted allegations that data broker Oracle invaded plaintiffs' privacy through its "ID Graph" identity resolution services and Data Marketplace—both functionally identical to those services offered by LiveRamp. In rejecting the same argument that LiveRamp makes here, that "the data allegedly collected was not sensitive [or private] in nature" and that plaintiffs had no expectation of privacy in their internet activity, the court stated: "Plaintiffs' strongest argument lies in its allegation that Oracle's accumulation of a 'vast repository of personal data'—from compiling Plaintiffs' browsing activity, online communications, *and* offline activity—is what contravenes the reasonable expectation of privacy. This is in line with the analysis provided in *Facebook Tracking*." *Katz-Lacabe*, 668 F. Supp. 3d at 942 (emphasis in original). This Court has interpreted *Facebook Tracking* in concert, noting that where data "revealed a person's internet activity with such specificity that Facebook and others would be able to determine a user's personal interests, searches, and habits on third-party websites, there were material questions of fact as to whether a reasonable individual would find the

information collected to be sensitive and confidential." *Ross v. AT&T Mobility, LLC*, 2020 WL 9848766, at *8 (N.D. Cal. May 14, 2020) (internal quotation marks omitted). Similarly, in *Brooks v. Thomson Reuters Corp.*, involving a data broker compiling cradle-to-grave profiles from disparate sources, the court held that "compiling bits of Plaintiffs' personal information scattered throughout the internet (and allegedly in non-public sources) into a dossier is a significant invasion of privacy," noting "[t]he Supreme Court has held that compiling disparate pieces of information about a person into a single dossier, even if the individual pieces of information are publicly available, constitutes a significant invasion of privacy." 2021 WL 3621837, at *9 (N.D. Cal. Aug. 16, 2021) (citing *U.S Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989)).

Even assuming everything in LiveRamp's profiles was otherwise publicly available, "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." *U.S. Dep't of Def. v. Fed. Lab. Rels. Auth.*, 510 U.S. 487, 500 (1994); *see also Brooks*, 2021 WL 3621837, at *9. In *Fed. Trade Comm'n v. Kochava, Inc.*, denying data broker (and LiveRamp competitor[7]) Kochava's motion to dismiss, the court noted that "Kochava allegedly provides its customers with vast amounts of essentially non-anonymized information about millions of mobile device users' past physical locations, personal characteristics (including age, ethnicity, and gender), religious and political affiliations, marital and parental statuses, economic statuses, and more." 715 F. Supp. 3d 1319, 1325 (D. Idaho 2024). The court emphasized that "[i]n doing so, Kochava does not merely sell 'bits and pieces' of data that are available through other lawful means. Rather, it sells 'data designed to give its customers a '360-degree perspective' on the unique traits of millions of individual device users.'" *Id.* The court, again relying on *Facebook Tracking*, found these allegations stated an "invasion of privacy—which is substantial both in quantity and quality." *Id.*

The allegations in these cases mirror LiveRamp's conduct here. *See, e.g.*, Section I.A., *supra*; FAC ¶¶ 13-38 (LiveRamp collects, compiles, and sells extensive and sensitive online *and* offline information on Plaintiffs.); ¶ 54 (LiveRamp's "comprehensive consumer profile surveillance services" "[b]uild 360-degree view profiles" of Plaintiffs and Class members."); ¶¶

[7] *See, e.g.*, *LiveRamp, Inc. v. Kochava, Inc.*, 2020 WL 2065696, (N.D. Cal. Apr. 29, 2020) (trademark dispute where LiveRamp and Kochava "offer[] similar services").

176, 193 (LiveRamp creates comprehensive dossiers based on extensive and sensitive online *and* offline data, which constitute "cradle-to-grave profiles.").

LiveRamp's arguments fail to overcome the clear weight of this analogous authority. Courts have repeatedly rejected LiveRamp's argument that a reasonable expectation of privacy only exists against a defendant who affirmatively represented it would not track users' activity, an argument which not only fails to comprehend the nature of the claims here, but turns privacy law on its head. *See Katz-Lacabe*, 668 F. Supp. 3d 928 (reasonable expectation of privacy against party plaintiffs were not in privity with); *Griffith*, 697 F. Supp. 3d at 971 (rejecting same argument, noting that a person who does not use TikTok "might be just as alarmed to find that TikTok is collecting her browsing data as a Facebook user would be to discover that Facebook tracks her conduct when she is logged out").

LiveRamp's arguments regarding third-party disclosures are similarly deficient. Plaintiffs allege they were not aware of and did not consent to LiveRamp's conduct as an unknown entity surveilling them. FAC ¶¶ 149-163. LiveRamp offhandedly cites to privacy policies of third parties that are extraneous to the FAC that it suggests rebut these allegations, but does not even seek judicial notice of such material. Mot at 11. Any arguments regarding such disclosures are not properly before the Court and must be rejected. *See Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001) ("extraneous evidence should not be considered in ruling on a motion to dismiss"). In any event, such disclosures are irrelevant where Plaintiffs are indisputably not in privity with the defendant and did not knowingly interact with it. *Katz-Lacabe*, 668 F. Supp. 3d 928; FAC ¶¶ 149-163.

LiveRamp's attempts to distinguish *Facebook Tracking* based on alleged differences in (1) disclosures, (2) amount of data, (3) nature of data, and (4) correlations, all fail both legally and factually. ***First***, the Ninth Circuit's holding in *Facebook Tracking* did not turn solely on Facebook's misrepresentations; rather, it focused on whether the data was sensitive and whether the manner of collection violated social norms, finding that compiling highly personalized profiles from comprehensive browsing histories was itself a privacy violation. 956 F.3d at 603-04. While misrepresentations may be probative of a reasonable expectation, *Facebook Tracking* did not find

they were a *necessary* condition. *Id.* ***Second***, the amount of data was relevant only insofar as it enabled comprehensive, persistent profiling—something LiveRamp's own practices mirror by creating persistent RampIDs that track individuals across digital and physical spaces using both online and offline data. *See id.* at 603, 605. ***Third***, the court also made clear that sensitivity arises from the aggregation itself as it reveals intimate associations and characteristics, which is precisely what LiveRamp's services are designed to do. *See id.* at 604 n.7. ***Finally***, LiveRamp's reliance on supposed 'pseudonymiz[ation]' to defeat the privacy claims is unavailing. LiveRamp's entire business model is predicated on correlating online data with real-world offline identifiers to create actionable, *non*-anonymous profiles; thus, the conduct at issue is precisely the type of 'correlation' that *Facebook Tracking* found to violate privacy expectations. *Id.*; *see* FAC ¶¶ 51-131.

LiveRamp's attempt to distinguish *Katz-Lacabe* based on quibbles with scale fails for similar reasons. The *Katz-Lacabe* court did not establish a numerical threshold for privacy violations; it applied *Facebook Tracking*'s principle that aggregating data into "vast repositories of personal data" violates reasonable expectations of privacy. 668 F. Supp. 3d at 942. Here, LiveRamp provides functionally identical services to Oracle's: tracking and identity resolution to create persistent identifiers linked to comprehensive behavioral profiles, and a data marketplace enabling the sale of sensitive personal information. The specific numbers of websites tracked (here a "mere" tens of thousands, as opposed to hundreds of thousands) is irrelevant when the underlying resulting privacy invasion is the same. *See* FAC ¶ 79 (LiveRamp tracking mechanisms on more than 21,000 websites "connect[ing] to over 92% of US consumer time spent online.").

LiveRamp's reliance on cases finding no reasonable expectation of privacy in certain types of discrete activity fails because these cases either predate *Facebook Tracking* or involve fundamentally different conduct. *Low v. LinkedIn Corp.* involved disclosure of users' profile viewing activity to other LinkedIn users—conduct that occurred within a social media platform where users expected their activity to be visible to other users. 900 F. Supp. 2d 1010, 1016-17 (N.D. Cal. 2012). *Folgelstrom v. Lamps Plus* involved an advertiser obtaining a plaintiff's home address and using it to send snail mail—a far cry from the comprehensive surveillance apparatus LiveRamp operates. 195 Cal. App. 4th 986, 989-92 (2011), *as modified* (June 7, 2011). The various cases

LiveRamp cites involving specific, limited data collection (Mot. at 9-10) are all distinguishable because they involved single types of data or limited collection practices, not the comprehensive aggregation of both online and offline data that LiveRamp performs. Those authorities, holding that there is no expectation of privacy in certain discrete types of information or suggesting that there is a limited expectation of privacy over certain types of internet activity,[8] are thus beside the point.

Finally, the inherent sensitivity of any particular piece of information is not dispositive of the existence of a privacy interest. *Cf.* Mot. at 10-13. As the California Attorney General has recognized, "seemingly innocuous data points, when combined with other data points across masses of data, may be exploited to deduce startlingly personal characteristics." 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at * 2 (citing studies). As such, the wrongful aggregation of masses of such data can itself constitute a privacy violation. *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 6466195, at *9 (N.D. Cal. Oct. 3, 2023) (recognizing that "a detailed dossier of information about an individual [], by virtue of its comprehensiveness, implicates privacy concerns" and that "[i]t would be perverse to hold an individual entitled to no protection where a company amalgamates many pieces of information about that individual's preferences on the grounds that revealing any one preference is no big deal"); *Facebook Tracking*, 956 F.3d at 599 (recognizing privacy interest in aggregation of "likes, dislikes, interests, and habits over a significant amount of time"). LiveRamp engages in such conduct. FAC ¶¶ 54-131.

2. Plaintiffs Have Alleged Highly Offensive Conduct

"Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956

[8] *Thomas v. Papa Johns Int'l, Inc.*, 2024 WL 2060140, at *1 (S.D. Cal. May 8, 2024) (interactions on single website); *Farst v. AutoZone, Inc.*, 700 F. Supp. 3d 222, 230 (M.D. Pa. 2023) (same); *Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (same); *Heeger v. Facebook*, 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020) (IP addresses); *U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (e-mail and IP addresses); *Saeedy v. Microsoft Corp.*, 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (collection of data from Microsoft browser only); *Smith v. Facebook, Inc.*, 745 Fed. Appx. 8, 9 (9th Cir. 2018) (certain health websites only). This same authority also recognizes privacy in internet activity. *Thomas*, 2024 WL 2060140, at *2 ("This is not to say there can never be a reasonable expectation of privacy over internet activity").

F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 287). "While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.*

As an initial threshold matter, the Ninth Circuit has instructed, and courts within this District (including this Court) have repeatedly recognized, that this question is, except in rare outlier cases, one for the jury, not the Court. "The ultimate question of whether [a defendant's] tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." *Id*. "Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *Lau v. Gen Digital Inc*., 2023 WL 10553772, at *6 (N.D. Cal. Sept. 13, 2023) (quoting *In re Facebook, Inc., Consumer Priv. User Profile Litig*., 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019)) (Tigar, J.). "Only if the allegations 'show no reasonable expectation of privacy or an insubstantial impact on privacy interests' can the 'question of [a serious or highly offensive] invasion [] be adjudicated as a matter of law." *St. Aubin v. Carbon Health Techs., Inc*., 2024 WL 4369675, at *12 (N.D. Cal. Oct. 1, 2024) (quoting *Hill*, 7 Cal. 4th 40) (Tigar, J.). Moreover, where, as here, defendants claim their data gathering practices are "routine commercial behavior" (Mot. at 15-17), dismissal is "particularly inappropriate . . . [because] Defendants are the only party privy to the true extent of the intrusion on Plaintiffs' privacy." *Hayden v. Retail Equation, Inc.*, 2022 WL 2254461, at *8 (C.D. Cal. 2022); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014) (rejecting "routine commercial behavior" defense because the "highly offensive . . . question is best left for a jury").

To the extent the Court engages in a threshold analysis, the weight of authority and extensive factual allegations in the FAC demonstrate the conduct is both highly offensive and egregious. No case has found that the pervasive level of surveillance Plaintiffs allege is not highly offensive or egregious, and none of the authorities LiveRamp cites come close to the scope of conduct at issue. LiveRamp's citations relate to *individual* modes of data collection, which Plaintiffs allege it *combines* (with yet more data) as part of its surveillance apparatus. Nor does any case address the combination of this data with *offline* activity. *See., e.g.*, FAC ¶¶ 51-112; *see In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (disclosure of Google

data only); *Low*, 900 F. Supp. 2d at 1025 (disclosure of users' LinkedIn profile viewing history only); *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021) (collection of app usage data only); *Hammerling v. Google, LLC*, 2024 WL 937247, at *3 (9th Cir. Mar. 5, 2024) (same); *Folgelstrom*, 195 Cal. App. 4th at 992 (collection only of plaintiff's address).[9] Courts have repeatedly rejected arguments that surreptitious tracking of internet activity is mere "routine commercial behavior." LiveRamp notes that in *Hubbard v. Google LLC*, 2024 WL 3302066 (N.D. Cal. July 1, 2024), the court "distinguished Facebook (and similar cases) because *Hubbard* did not involve 'secret or deceptive data collection'"—but that is precisely what Plaintiffs allege here: the surreptitious collection of Plaintiffs' data in real time, across their devices, combined with an extensive digital dossier. FAC ¶¶ 51-112. As in *Katz-Lacabe*, such allegations "go well beyond the 'routine commercial behavior' of collecting contact information for sending advertisements." 668 F. Supp. 3d at 942 (distinguishing *Folgelstrom*).

LiveRamp also ignores Plaintiffs' extensive allegations that LiveRamp's challenged conduct has been repeatedly recognized as highly offensive since its inception. LiveRamp's surreptitious tracking and correlating of online activity with real-world offline identities and personal information has been decried as "creepy" and "evil," with LiveRamp described as a "Privacy Death Star" and "like a stalker, who gradually learns more about the target, but it's highly automated, at population scale, and it sells this stalking ability to many other companies." FAC ¶¶ 11, 56, 132-148. Privacy advocates have filed formal complaints against LiveRamp with regulators in multiple countries, describing LiveRamp's practices as "more intrusive and pervasive than previous adtech technologies." FAC ¶¶ 148. The FTC sued LiveRamp's business partner for illegally selling browsing data to LiveRamp without users' knowledge or consent, noting that such "re-identifiable browsing information" is "sensitive data" and that users were harmed by LiveRamp's collection of that information. FAC ¶¶ 146-147. The extensive public criticism,

[9] *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) and *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) predate *Facebook Tracking* and are outdated, and have subsequently been found "unpersuasive" due to their "lack of consideration for California's privacy norms." *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018) (citing *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1079 (N.D. Cal. 2016).

regulatory action, and commentary detailed in Plaintiffs' complaint establishes that the community norm rejects LiveRamp's comprehensive surveillance activities as highly offensive.

3. The CCPA Does Not Foreclose Plaintiffs' Privacy Claims

LiveRamp's assertion that the CCPA immunizes its conduct is refuted by the statute's language and numerous courts. The CCPA unambiguously states that it was "intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information," and that "in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control." Cal. Civ. Code § 1798.175. LiveRamp fails to cite a single case supporting its quasi-preemption defense, which every court to have addressed has rejected, finding it "meritless." *Brooks*, 2021 WL 3621837, at *6 (rejecting argument that defendants' conduct could not be "unfair' under the UCL because it was "expressly permitted by" the CCPA); *Mirmalek v. Los Angeles Times Commc'ns LLC*, 2024 WL 5102709, at *5 (N.D. Cal. Dec. 12, 2024) (rejecting argument that CCPA "should control" because application of stricter privacy laws would "supplant . . . the detailed notice and 'opt out' framework of the CCPA"); *Kellman v. Spokeo, Inc.*, 599 F. Supp. 3d 877, 897 (N.D. Cal. 2022) (rejecting defendant's argument that it could not be liable under California's UCL because the CCPA contained an "expressed exemption" for its conduct, finding the CCPA does not "expressly or impliedly set aside privacy-based tort claims"). LiveRamp's argument turns the law's purpose on its head—the CCPA was not intended to create an affirmative defense for surveillance companies against longstanding privacy rights, and its findings expressly condemn "advertising businesses [that] use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles," Cal. Prop. 24 (2020) § 2(I), precisely describing LiveRamp's invasive conduct that California voters sought to curtail, not bless.

4. LiveRamp's Data Marketplace Arguments Fail

As a threshold matter, and as with LiveRamp's arguments excluding Attribute Enrichment, even were LiveRamp's Data Marketplace-related arguments successful, they still would not dispose of the entirety of the invasion of privacy claims because they are only directed at those claims "to

the extent [they] arise out of the operation of Data Marketplace." Mot. at 2. Plaintiffs allege that LiveRamp's RampID-based identity profiles, independent of any interaction with the Data Marketplace, violate their privacy. FAC ¶ 94 ("LiveRamp's identity profiles and their uses as described above, standing alone, violate Plaintiffs' privacy rights"). Since the invasion of privacy claims encompass conduct beyond the Data Marketplace, LiveRamp's arguments cannot provide grounds to dismiss these claims in their entirety, and can be disregarded for that reason alone.

LiveRamp incorrectly contends that Plaintiffs challenge the "mere" operation of a data marketplace and that California law's contemplation of data markets precludes any privacy violation. Mot. at 17. However, Plaintiffs allege that the Data Marketplace enables the sale and distribution of highly sensitive and aggregated personal information—including health, financial, political, and behavioral data—without notice or consent, going well beyond routine commercial conduct. FAC ¶¶ 94-131, 149-163. The FAC provides extensive detail about how the Marketplace facilitates the construction and sale of these profiles that go far beyond routine commercial activity, detailing dozens of specific, highly sensitive segments sold on the Data Marketplace—including those relating to reproductive health, sexual orientation, financial distress, and political views. FAC ¶¶ 97-104, 118-126 (citing segments such as "Condom Buyer," "Addictions > Sex," "Consumer has Requested a Payday Loan," "Sociodemographics > Gamblers," "Transgender Bathroom Rights > Opponents," and others). LiveRamp's assertion that the allegations about sensitive segments are "threadbare and conclusory" ignores this extensive factual development. *See id.*

Likewise, LiveRamp's attempt to invoke Section 230 fundamentally miscasts the nature of Plaintiffs' claims and LiveRamp's role in the misconduct. A defendant must establish to obtain Section 230 immunity: "(1) [it is] a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 681 (9th Cir. 2019). LiveRamp cannot satisfy the second or third prongs. To begin, it is nothing like social media platforms, physical product sales websites, or advertisement-listing services in the cases it relies on granting immunity. "The prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post

comments and respond to comments posted by others." *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016) (quotations omitted). LiveRamp is a data broker. Plaintiffs challenge its *collection and aggregation* of personal data on the Data Marketplace, combined with identity resolution, as privacy invasive. Their claims do not rely on the invasiveness of the dissemination of any particular piece of information. Section 230 is simply not a good "fit" for this conduct. Courts that have confronted data brokers' analogous attempts to invoke Section 230 have rejected the defense as trying "to fit square peg into a round hole." *F.T.C. v. Accusearch*, 2007 WL 4356786, at *3 (D. Wyo. Sept. 28, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009); *see also Brooks*, 2021 WL 3621837, at *13. The same result is compelled here.

Plaintiffs do not seek to hold LiveRamp liable for third-party speech or for exercising editorial functions. Instead, they challenge LiveRamp's own commercial conduct: the creation, curation, packaging, and sale of dossiers consisting of "bespoke audiences," RampID-linked identity graphs, and psychographic profiles comprising data from the Data Marketplace, which LiveRamp itself develops, markets, and monetizes. As in *Brooks*, Plaintiffs "are not asking [the defendant] to monitor third-party content; they are asking to moderate its own content." 2021 WL 3621837, at *13. No editorial-function immunity is implicated when the defendant is responsible for creating the content at issue. Even if it were arguably a publisher or speaker of others' content, immunity evaporates because LiveRamp is "responsible, in whole or in part, for the creation or development of" the information at issue. *See* 47 U.S.C. § 230(f)(3) (defining "information content provider"). The FAC documents that *LiveRamp* constructs the RampIDs; *LiveRamp* engineers the "identity graph;" *LiveRamp* requires Marketplace participants to purchase its identity-resolution services, without which the data have no commercial utility; *LiveRamp* markets its own "bespoke" or "custom" segments; and *LiveRamp* directly sells "Attribute Enrichment" packages that deliver customized profiles utilizing Marketplace data. FAC ¶¶ 108-110, 113-131. These allegations place LiveRamp well outside the "heartland" of Section 230 immunity for mere platforms that publish third-party speech. *Cf.* Mot. at 18 (citing *Gonzalez v. Google LLC*, 2 F.4th 871, 891 (9th Cir. 2021)).

Those facts also mirror the allegations that defeated immunity sought by data brokers in *Accusearch* and *Brooks.* In *Accusearch*, the defendant "advertised the availability of phone records,

solicited orders, purchased the records from third-party sources for a fee, and then resold them to the end-consumers." 2007 WL 4356786, at *5. Section 230 was unavailable because in so doing the defendant "participat[ed] in the creation or development of [the] information." *Id*. Likewise, *Brooks* rejected immunity where Thomson Reuters curated and sold dossiers drawn from multiple third-party sources, explaining that Section 230 "immunize[s] the removal of user-generated content, not the creation of content." 2021 WL 3621837, at *13. LiveRamp's conduct is indistinguishable: it "actively take[s] content from other sources, curate[s] it, and upload[s] it . . . in a novel configuration for repurposed uses," *Kellman*, 599 F. Supp. at 898, and thus falls outside the statute. FAC ¶¶ 113-131.

Plaintiffs' amended allegations—quoting LiveRamp's own statements that it "creates" "bespoke" and "custom" information for clients—definitively resolve any question about Section 230 immunity. As the FAC explains, in late 2024, Oracle shuttered its ad tech and data brokering business, shortly after settling a lawsuit filed by privacy advocates alleging Oracle had engaged in large-scale illegal surveillance through its ad tech practices. FAC ¶ 129. A central product offering was "Oracle Audiences," which were "curated" datasets "built and acquired" directly by Oracle. *Id.* As Plaintiffs allege, "LiveRamp wasted no time assuring former Oracle clients that the 'LiveRamp Data Marketplace offers a seamless transition to those clients looking for alternatives to Oracle's [data] offerings . . . . [t]o facilitate a smooth transition from Oracle Branded Audiences and Audiences by Oracle, we've developed *bespoke* third-party data audiences *tailored to your specific needs*.'" *Id.* ¶ 130 (emphasis added). LiveRamp states that it "[i]f a customer doesn't have a specific segment or dataset in mind, or it isn't available in the Data Marketplace, LiveRamp can *create* custom segments specifically for a campaign or advertiser." FAC ¶ 128. LiveRamp—in its own words—*creates* content utilizing Data Marketplace data. That is the end of the matter.

LiveRamp's argument that, even if it is a content creator, it can only be liable if it is engaged in creating specifically offensive conduct has no basis in law. Section 230 immunity does not apply so long as the defendant is "responsible, in whole or in part, for the creation or development of" the information at issue. 47 U.S.C. § 230(f)(3). LiveRamp's attempt to analogize its operations to Airbnb's platform misses the mark. In the *Airbnb* case, Section 230 immunity was found because

Airbnb provided a neutral platform where third parties posted their own content. *La Park La Brea A LLC v. Airbnb, Inc.*, 285 F. Supp. 3d 1097, 1105 (C.D. Cal. 2017). In contrast, as alleged in paragraphs 113–131 of the FAC, LiveRamp plays (and holds itself out to investors as playing) an active and central role in the creation, curation, "match[ing]" and "activat[ing]," of the information issue, and in fact Data Marketplace data is useless unless it is packaged with LiveRamp's own extensive and privacy-invasive identity profiles. *Id.* This is far more than "merely provid[ing] a framework that could be utilized for proper or improper purposes." *La Park La Brea A LLC*, 285 F. Supp. 3d at 1105. As such LiveRamp "contributes materially to the alleged illegality of the conduct." *Id.* at 1103. Courts have consistently held that Section 230 immunity does not extend to entities that actively shape, create, or develop the content at issue, or that require the use of illegal tools to make information usable. *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157 (9th Cir. 2008). LiveRamp's tight integration of identity resolution, curation, content creation, and "activation" is the antithesis of a passive conduit. Section 230 immunity does not apply.

C. Plaintiffs State Claims Under CIPA and the ECPA (Counts III & IV)

1. Purported Client Consent Does Not Defeat the ECPA Claim

Regardless of any purported client consent,[10] Plaintiffs plausibly allege LiveRamp acted "for the purpose of committing any criminal or tortious act" under 18 U.S.C. § 2511(2)(d), which provides an exception to one-party consent. *See* FAC ¶¶ 253-56 (alleging interceptions were performed for purposes violating Plaintiffs' privacy). Plaintiffs' allegations are sufficient to invoke the ECPA's crime-tort exception. *See, e.g., Brown v. Google*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (allegation defendant intercepted communications for associating data with preexisting user profiles in violation of plaintiffs' privacy sufficient to invoke crime-tort exception); *Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016) ("defendants' subsequent disclosure of the contents of the intercepted conversations for the alleged purpose of *further* invading the privacy of plaintiffs' staff satisfies" the exception).

[10] LiveRamp incorrectly reasons that in the absence of any contrary allegation in the complaint, one must infer that LiveRamp's clients' consented to the misconduct. *See* Mot. at 20. Not so. LiveRamp – not Plaintiffs – bears the burden of proving this affirmative defense. *See, e.g., Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1078 (N.D. Cal. 2023).

Under Ninth Circuit law, any purported legitimate purpose that LiveRamp may now assert does not "sanitize" an interception that was also made for a tortious purpose. *Sussman v. Am. Broad. Cos., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999). LiveRamp's reliance on *Katz-Lacabe* for this point is misplaced, as several courts have subsequently expressly disagreed with its finding that the goal of "mak[ing] money" immunizes a tortfeasor from ECPA liability. *In re Grp. Health Plan Litig.*, 709 F. Supp. 3d 707, 720 (D. Minn. 2023) (disagreeing with *Katz-Lacabe*); *see also R.S. v. Prime Healthcare Servs., Inc.*, 2025 WL 103488, at *7 (C.D. Cal. Jan. 13, 2025) (joining "those courts that have held a monetary purpose does not insulate a party from liability under the ECPA"); *Castillo v. Costco Wholesale Corp.*, 2024 WL 4785136, at *6 (W.D. Wash. Nov. 14, 2024) ("the crime-tort exception applies even when a defendant intercepts data for the purpose of financial gain"); *Stein v. Edward-Elmhurst Health*, 2025 WL 580556, at *5-6 (N.D. Ill. Feb. 21, 2025) ("criminal or tortious" modifies "act" not "purpose" and any other interpretation would erroneously "import a *mens rea* element into the statute"). Courts have repeatedly found the exception applies where the further use of the intercepted data was in violation of the right to privacy. *See, e.g.*, *Brown*, 525 F. Supp. 3d at 1067 (allegations of common law invasion of privacy sufficient to apply the crime-tort exception); *R.C. v. Walgreens*, 733 F. Supp. 3d 876, 901-02 (C.D. Cal. 2024) (same); *B.K. v. Desert Care Network*, 2024 WL 1343305, at *5 (N.D. Cal. Feb. 1, 2024) (same). Because Plaintiff's privacy claims include the predicate tortious acts, including the further use of the fruits of the interceptions, the exception applies here.

2. Plaintiffs' Allegations Satisfies CIPA's "While In Transit" Requirement

CIPA liability attaches when a defendant "reads, or attempts to read, or to learn the contents" of a communication while it "is in transit . . . or is being sent from, or received at any place within" California. Cal. Pen. Code § 631(a). LiveRamp argues Plaintiffs cannot establish CIPA's "while . . . in transit" element because CIPA requires a "showing of real-time interpretation." Mot. at 21. According to LiveRamp, such a showing is impossible because Internet communications travel "much too fast to permit real-time review." *Id.* at 22.[11] LiveRamp is wrong as a matter of fact and law. On the facts, Plaintiffs allegations show contemporaneous reading and

[11] LiveRamp's argument is, in effect, an invitation to make (inaccurate) factual assumptions about the technological processes at play. Such attempts are inappropriate on a motion to dismiss.

interpretation of communications, explicitly describing simultaneous interception and reading. *See, e.g.*, FAC ¶ 79 ("Event listeners intercept communications while in transit, once user inputs are made but before the communications are received by the webpage."); *Id.* at ¶ 217 (LiveRamp uses "'event listeners' to detect specific types of contents of communications . . . and intercept those contents and *simultaneously* transmit them to LiveRamp.") (emphasis added); *Id.* at ¶¶ 207-247, *passim*. Moreover, a central component of the misconduct is LiveRamp's ability to ingest, analyze, and connect intercepted data points into user profiles for the *immediate* tracking of a user. *See, e.g.*, *id.* at ¶ 3 (real-time inferences and updating of user profiles), ¶ 6 (identity graph connects "identifying points of data . . . . to a real person *that can be used to track all of that person's online activity in real time*") (emphasis added), ¶ 87 (immediate reading and information usage so as to serve targeted advertising "based on [] real-time physical locations"), ¶ 90 (use in *real-time* bidding advertising). These allegations are sufficient under CIPA. *See, e.g.*, *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023) (crediting allegations of real-time interception at the pleadings stage).[12]

LiveRamp primarily relies on *Torres v. Prudential Fin., Inc.*, 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025), which is procedurally and factually distinguishable. *Torres* was decided on a motion for summary judgment, only after the development of a full factual record, rather than at the pleadings. Indeed, the claim *survived* the defendants' motion to dismiss. *Hazel*, 2023 WL 3933073, at *3. On the merits, Judge Breyer found that the undisputed evidenced showed the defendant recorded communications but *never* attempted to read them or learn their substantive meaning. 2025 WL 1135088, at *5. The *Torres* defendant was a provider of TCPA compliance software, which documented whether website visitors filled out a webform consenting to be contacted by the website owner. *See Torres*, No. 22-cv-07465, MSJ (ECF 93 at 2-3) (Nov. 15, 2024). When a visitor filled out the form, the defendant generated a "certificate" to document the consent. *Id.* at 3. The defendant stored the certificate on behalf of the website in an encrypted form that was not analyzed as a matter of common business practice. *Id.* at 6; *Torres*, 2025 WL 1135088, at *1. In other words, there was no evidence the defendant ever attempted to do anything but *record* the communication,

[12] LiveRamp claims *Hazel* (sub nom *Torres*) dismissed the CIPA claim. Mot. at 21. This is incorrect

only evidence that the defendant's employees *could* potentially access information *after* it was stored on the servers. *Torres*, 2025 WL 1135088, at *5-6. Judge Breyer held that a hypothetical future attempt to understand the meaning of a communication was insufficient, and distinguished those facts from an eavesdropper (like LiveRamp) who "track[s] users' browsing histories, which it then use[s] to create personal profiles that [can] be sold to advertisers," 2025 WL 1135088, at *6 (citing *Facebook Tracking*, 956 F.3d at 596). In such circumstances, "CIPA remains perfectly viable in the context of internet communications." *Id.* at n.5. LiveRamp's statement that *Torres* "acknowledged that the read-in-transit requirement makes it difficult to establish Section 631(a) violation in the context of the internet," is thus untrue; the court in fact rejected that argument. *Torres*, 2025 WL 1135088, at *6.[13]

Unlike *Torres*, LiveRamp read the intercepted communications while in transit. *See supra*. LiveRamp is incorrect that *Torres* brings "event listeners"— code that intercepts and interprets communications with websites in real time—outside CIPA as a matter of law. Mot. at 22. The defendant in *Torres* hashed Plaintiffs' emails and phone numbers without any attempt to analyze the underlying information. 2025 WL 1135088, at *7. LiveRamp uses event listeners to intercept Plaintiffs' contact information, link them to a browsing session and internal profile, and broadcast the information to tens of thousands of advertisers. FAC ¶¶ 240-43. These circumstances are starkly different than those in *Torres*. In any event, the exact technical details of LiveRamp's conduct, including timing, are "a question for summary judgment." court. *Hazel*, 2023 WL 3933073, at *4.

3. LiveRamp's Technologies are "Pen Registers" under CIPA[14]

CIPA defines "pen register" and "trap and trace" devices as devices or processes that capture "dialing, routing, addressing, or signaling information" relating to "a wire *or electronic* communication, but not the contents of a communication." Cal. Pen. Code § 638.50 (emphasis added). LiveRamp erroneously argues CIPA does not apply to "tracking or recording

[13] LiveRamp's other cited authorities are distinguishable. *See Williams v. DDR Media*, 757 F. Supp. 3d 989 (N.D. Cal. 2024) (another TCPA compliance software *summary judgment* decision, where data was immediately hashed and thus incomprehensible); *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751 (N.D. Cal. 2023) (plaintiff's timing allegations too conclusory); *Love v. Ladder Financial*, 2024 WL 2104497, at *1 (N.D. Cal. May 8, 2024) (failed to allege timing element at all); *James v. Allstate Ins.*, 2023 WL 8879246, at *3 (N.D. Cal. Dec. 22, 2023) (same).

[14] Plaintiffs do not oppose LiveRamp's request for judicial notice (Dkt. 50).

activity on the internet," (Mot. at 23), but the statute expressly extends protection to Internet communications through *both* "wire" *and* "electronic communications." Had the statutory intent been limited to telephone communications, there would be no need for additional definitions. Because the 2015 California pen register statute adopted the same definition as the federal Pen Register act (which was amended in 2001 to apply "to a wide array of mode[rn] communications technologies, such as the Internet," *In re Certified Question of L.*, 858 F.3d 591, 603 (Foreign Intel. Surv. Ct. Rev. 2016)), a plain language analysis of CIPA confirms the scope of the claim.

While LiveRamp points to two state court decisions supporting its position, it acknowledges that federal courts have *unanimously* rejected challenges to analogous pen register claims.[15] These courts have recognized that "[t]he Court's task is to interpret the law as the Legislature wrote it" and "the pen register statute is broadly written, and under California law, is to be interpreted broadly to protect privacy and to be applied to new techniques and technologies." *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 932-33 (N.D. Cal. 2024). Finally, LiveRamp's rule of lenity argument fails because the rule applies "only if the court can do no more than guess what the legislative body intended; there must be an egregious ambiguity and uncertainty to justify invoking the rule." *People v. Superior Ct. of Riverside Cnty.*, 81 Cal. App. 5th 851, 8886 (2022). There is no such egregious ambiguity here.

D. Plaintiffs Have Properly Alleged Unjust Enrichment

LiveRamp's perfunctory challenge focuses solely on pleading adequacy rather than disputing unjust enrichment as a cognizable standalone claim. Plaintiffs have adequately pled the two elements of unjust enrichment under California law: "receipt of a benefit and unjust retention of the benefit at the expense of another." *James Williams v. VISA, Inc.*, 2025 WL 1518044, at *5 (N.D. Cal. May 28, 2025) (Tigar, J.). LiveRamp has "unjustly profited from tracking, disclosing, and profiting from Plaintiffs and U.S. Class members' internet activity and real-world activity to third parties without [their] knowledge or consent," conferring benefits "at the expense" of their

[15] *See* Mot. at 24 (citing *Shah v. Fandom*); *Zarif v. Hwareh.com, Inc.*, 2025 WL 486317, at *4 (S.D. Cal. Feb. 13, 2025); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023); *Conohan v. Rad Power Bikes Inc.*, 2025 WL 1111246, at *6 (C.D. Cal. Apr. 3, 2025); *see also Mirmalek v. LA Times*, 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024); *Lesh v. CNN, Inc.*, 767 F. Supp. 3d 33 (S.D.N.Y. 2025); *Rodriguez v. Autotrader.com, Inc.*, 762 F. Supp. 3d 921 (C.D. Cal. 2025); *Heiting v. FKA Distributing Co.*, 2025 WL 736594 (S.D. Cal. Feb. 3, 2025).

privacy rights. FAC ¶¶ 259-76. This aligns with Restatement (Third) of Restitution and Unjust Enrichment § 44, which recognizes that "profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement." California law does not require corresponding financial loss, as held in *Facebook Tracking*, recognizing "a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss." 956 F.3d at 599. This Court has consistently applied this principle in data privacy cases, holding plaintiffs may pursue "unjust enrichment to recover the gains [defendants] realized" from [their] allegedly improper conduct" though plaintiffs "suffered no economic loss." *Lau*, 2023 WL 10553772, at *7; *see also Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 604-05 (N.D. Cal. 2021) (Tigar, J.). Moreover, "California law imposes no requirement of privity to make out an unjust enrichment claim." *In re Gen. Motors LLC CP4 Fuel Pump Litig.*, 393 F. Supp. 3d 871, 882 (N.D. Cal. 2019).

The progression of the *Katz-Lacabe* case directly supports this claim: while initially dismissing the claim, upon amendment with facts saliently identical to those alleged here, the court allowed unjust enrichment to proceed, confirming that "Oracle's collection of data from third-party websites . . . conferred a benefit upon Oracle at the expense of the privacy of [plaintiffs'] data." *Katz-Lacabe*, 2023 WL 6466195, at *6; *see also Brooks*, 2021 WL 3621837, at *12 (unjust enrichment claim allowed against data broker for creating "detailed cradle-to-grave dossiers" using third-party data). LiveRamp's conduct is functionally identical to Oracle's, and, particularly given LiveRamp's posture as Oracle's self-proclaimed successor (FAC ¶¶ 129-131), Plaintiffs are likewise entitled to unjust enrichment.

E. Plaintiffs Have Properly Alleged a Claim for Declaratory Relief

As with Counts I and II, LiveRamp's failure to challenge the entirety of this claim necessitates denial of its motion. Because LiveRamp's other arguments fail, this claim survives.

III. CONCLUSION

Plaintiffs respectfully submit that the Court should deny LiveRamp's motion in its entirety, but that any dismissal, in whole or in part, should be without prejudice and with leave to amend.

Dated: June 16, 2025

Respectfully Submitted,

Michael W. Sobol
Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Jason "Jay" O. Barnes
Jason "Jay" O. Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
An V. Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
12 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Attorneys for Plaintiffs and the Proposed Classes

ATTESTATION

Pursuant to Civil Local Rule 5.1 regarding signatures, I attest that concurrence in the filing of this document has been obtained from the other signatories.

Dated: June 16, 2025

Michael W. Sobol
Michael W. Sobol
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP